From: DEBO Jurgen
To: Microsoft ATR
Date: 12/6/01 2:04pm
Subject: Tip for better solution for the discussion

Dear Justice Office,

I am programmer for 20 years, and CEO of an IT company.
My english is very bad, but it is the thought I wish to tell.

For the moment there is a high focus on terrorism. But what huge terrorism doesn't we have on internet, or by software that is violating our privacy and our common data.

We can not denyn, in future, we will be forced to switch over to open source software. When companies are doing E-Business, no company wants that statistics are made based on his activities, done by a software developer. When software is not open, you can not watch in the black box what is hidden behind. On the other side, companies needs to live from software. But it is widly known that microsoft software has a lack of security, a lack of privacy and that microsoft is sneeping inside computers.

A good option would be that all elements communicating with the outside, like browsers, components, firewalls, e-mail clients etc should be open source by federal law. Just like the known history of PGP (Pretty good privacy) (It was and is still open source.) This should be a barrier arround the black box.

Black boxes are fine for home use, but when they make outside communications, this is dangerous. So if there is still a kernal part running on themselves, without making communications, that's maybe ok for the moment, but communicating particles needs to be open source, that's our right of privacy, and protecting of our own data. Every communicating particle should be explained clearly to public what it is sending out, with a technical sheet, to verify if this is correct for (intrusion detection software, like the open source project www.snort.org)

Secondly, every communication should have an identification header of the number of the CPU so it can be traced down by Law Organisations. Every sold CPU should be registered in a huge internet security company. That ID should be integrated into the IP protocol, encrypted and coded with a high protection, and only viewable by those offices. This would identify malifious people, who doing all non-legal practices, like terrorism, abuse of children, drugs, hacking of computers, etc etc.

Without those steps E-Commerce will NEVER be possible on a professional, worldlevel schedule. There are too much violations due to people who

make profits of the gray zone of unknown, to be on internet and the gray zone of hidden gateways in our software.

If my idea's are worthfull, please consider to invest in our directory engine as return for this information.

Sincerely,

Jurgen Debo
CEO
Belgian Directory
The Guide www.guide.be